IV. Emergency Mode Operation Plan

A. The Emergency Mode Operation Plan must enable the Department to continue its operations and business processes in the event of fire, vandalism, systems failure, or other disaster, and must safeguard the security of data. Regardless of the scope of the emergency, the Emergency Mode Operation Plan provides for emergency operations. If the emergency is limited to a server failure, the Emergency Mode Operation Plan may provide direction to use another server somewhere in the facility. If it is a DMH-wide emergency, the Emergency Mode Operation Plan may require operations be performed from another location until the disaster/emergency is over.

B. In creating this Plan, include all of the following:

a. Base the Plan on the criticality analysis for each IT information system.

b. Focus on the recovery of operations and business continuity rather than recovery of electronic record and data sets. Some electronic records and data sets may have to be recovered to permit the continuity of operations.

c. Identify the scope, including the severity of the emergency (e.g., system only, facility-wide, DMH-wide) and the duration of the emergency (e.g., until repair, day, week, month, undetermined).

d. Identify type of recovery (e.g., hot site, warm site, cold site, disk mirroring) that is required by the scope of the emergency.

e. Identify emergency continuity personnel, including either backup personnel or personnel cross-trained to assure adequate staffing in the event of an emergency.

f. Designate specific roles and responsibilities to initiate and maintain emergency mode operations including information system and security personnel.

g. Include the following emergency access control requirements:

i. Determine emergency access control requirements for emergency mode operations and ensure that the access control matrices reflect such requirements.

ii. Give users additional privileges in the event of a crisis situation to access information as needed and in accordance with the above emergency mode operation procedures.

C. Create the Emergency Operation Mode Plan spreadsheet:

a. From the Application and Data Criticality Analysis spreadsheet (Attachment I), copy the Official System Name, System Owner, and Director Priority Level columns into a new spreadsheet.

b. Add columns for Scope of Emergency, Level of Emergency, Type of Recovery, Facility Access, and System Access to create the DMH Emergency Operation Mode Plan spreadsheet, shown below:

DMH EMERGENCY MODE OPERATION PLAN

Date:

Official System Name	System Owner	Director's Priority Level	Scope of Emergency	Level of Emergency	Type of Recovery	Facility Access	System Access

c. Complete the spreadsheet by filling in all of the data.

i. In the Scope of Emergency column, define the breadth and extent of the emergency. It may be a system emergency (e.g., loss of mainframe, server, client, or peripheral device like router, switch, hub, or printer); a facility emergency (e.g., loss of a room, floor, loss of utility services to a facility, building), or group of a DMH emergency (e.g., loss of an enterprise-wide application, networking infrastructure, communication infrastructure); or a County emergency (e.g., loss of countywide electricity, telephone, or other communications).

ii. In the Level of Emergency column, enter one of the following three levels:

- Level 1 Emergency Operations: Local, day to day, involving the loss of a location or function
- Level 2 Emergency Operations: An incident affecting multiple locations or functions
- Level 3 Emergency Operations: Major disruption to one or more locations or functions

iii. In the Type of Recovery column, define both the (1) locations and (2) recovery methods. An actual location or specific system location will be specified (e.g., hot site; disk mirroring).

(1) Continuity Locations

A continuity location is the place DMH can use to recover the Department's operation(s) in the event of an emergency or disaster. An internal site is a continuity location within DMH or the County. An external site is a location that does not belong to DMH or the County. Examples of the types of locations and data recovery methods are:

- A hot site is a data center facility that is configured with the hardware and network communications required to recover the Department's operation. The location must be environmentally controlled and available to the Department upon a declaration of disaster.
- A warm site is a data center facility that contains HVAC, electrical power, network communication for voice and data access, and some hardware available to use for recovery.

- A cold site is a data center facility equipped with HVAC, electrical power, and network communications for voice and data. A cold site has no hardware available to use for recovery.

(2) Data Recovery Methods

- Electronic vaulting writes backup tapes over the network to the recovery site. The recovery point objective is shortened because the data that is used is more current than the standard 24-hour off-site storage process.

- Electronic journaling writes transactions and journals over the network to a second location. The information can then be restored on other systems at a hot site. This process diminishes the amount of data lost in the event of an emergency at the primary facility.

- Disk shadowing and mirroring allows for data replication to remote disks. Shadowing is asynchronous; there is a lag between the primary system and the replaced system. Synchronous mirroring means the data sent to the secondary system is current with the primary system.

- A hot standby is a replicated server waiting to take the processing load. The hot standby may be load balanced between the primary operating site and a second location to ensure both systems are up-to-date.

iv. In the Facility Access and System Access columns, enter a Yes or No notation. For each type of recovery, "Yes' means that secure access for emergency personnel has been provided to both the facility and system recovery site or method.

D. In implementing this Plan, include both of the following tasks:

a. Implement the emergency access requirements in section B. a. above.

b. Test the emergency mode operation procedures as set forth in Attachment VI.